ABSTRACT

A method and apparatus for an iterative cryptographic block under the control of a CPU and without a fixed number of stages. In one embodiment, a first cryptographic block descrambles received information using an internal key or a preprogrammed key to form a descrambled key or descrambled data. A data feedback path stores the descrambled data as internal data and provides the internal data or the external data as data input to the first cryptographic block. A key feedback path stores the descrambled key as an internal key and provides the internal key or the preprogrammed key to a key input of the first cryptographic block. A second cryptographic block descrambles received content using a final descrambling key. Other embodiments are described and claimed.